

РЕЦЕНЗИЯ

върху дисертационен труд за придобиване на образователна и научна степен „доктор“

по професионално направление 5.3. „Комуникационна и компютърна техника“, научна специалност „Автоматизация на инженерния труд и системи за автоматизирано проектиране“

Автор на дисертационния труд:

Маг. Ериселда Малай

Тема на дисертационния труд:

Разработване на нови хардуерни решения за киберсигурност на комуникационни системи

доц. д-р инж. Адриана [] Бороджиева

Русенски университет „Ангел Кънчев“, факултет „Електротех-ника, електроника и автоматика“, катедра „Телекомуникации“
гр. Русе – 7017, ул. „Студентска“ № 8

1. Актуалност на разработвания в дисертационния труд проблем в научно и научно-приложно отношение. Степен и нива на актуалността на проблема и конкретните задачи, разработени в дисертацията

Дисертационният труд е посветен на разработването и оценката на нови хардуерни решения за киберсигурност на комуникационни системи чрез логическо криптиране на ниво схема. Изследването разглежда три основни подхода за логическо криптиране – XOR/XNOR-базирано, MUX-базирано и Flip-Flop-базирано – и анализира тяхната ефективност, устойчивост на атаки и приложимост в комуникационно-ориентиран хардуер.

Актуалността на темата се определя от няколко ключови фактора:

- **глобализираното производство на интегрални схеми**, което увеличава риска от пиратство, свръхпроизводство и подмяна на интелектуална собственост;
- **реалните хардуерни заплахи**, включително reverse engineering, fault injection, side-channel анализ и SAT-базирани атаки, които заобикалят традиционните софтуерни механизми за защита;
- **нарастващата необходимост от защита на хардуерно ниво** в комуникационни, вградени и критични системи, където компрометиране на хардуера води до сериозни функционални и сигурностни последствия.

В дисертацията е формулиран ясен научен фокус: логическото криптиране като средство за защита на цифрови комуникационни схеми. Изследването поставя акцент върху:

- функционална обфускация, оценена чрез Average Hamming Distance (AHD);
- устойчивост на грешки и атаки, измерена чрез Average Fault Sensitivity (AFS) и fault-based анализ;

- SAT-устойчивост на криптираните архитектури;
- хардуерни показатели като мощност, площ и закъснение;
- алгоритъм за вземане на решения при внедряване (deployment decision) за FPGA и ASIC платформи според измерените метрики.

Проблемът е научно и научно-приложно значим, тъй като стъпва върху утвърдени теоретични основи – логическо заключване, SAT атаки, ISCAS бенчмаркове – и води до практически насоки за защита на реални комуникационни подсистеми.

Структурата на дисертацията е логична и последователна:

Глава 1 представя задълбочен обзор на съществуващата литература в областта на хардуерната сигурност, логическото криптиране и обфускацията, като очертава пропуските в съвременните подходи.

Глава 2 описва теоретичната основа, моделите на атаки и използваната научна методология, включително метрики за сигурност и проектни инструменти.

Глава 3 разглежда проектирането и реализацията на криптиращите модули, архитектурните решения и стратегиите за управление на ключове.

Глава 4 представя средата за симулация, използваните бенчмаркове и резултатите от оценяването на сигурността и хардуерните показатели.

Глава 5 анализира получените резултати, оценява компромисите между сигурност и хардуерна ефективност и разглежда устойчивостта на предложените техники срещу различни видове атаки.

Заключението обобщава основните приноси и очертава насоки за бъдеща работа, включително въпроси, свързани с мащабируемостта и защитата на интегрални схеми от следващо поколение. Приложенията съдържат допълнителни материали, програмен код и експериментални данни, които подкрепят основното изследване.

Формулираните цели и задачи са последователни, научно обосновани и напълно съответстват на актуалните тенденции в хардуерната сигурност. Всичко това определя високата научна и научно-приложна значимост на разглеждания проблем.

2. Степен на познаване състоянието на проблема и творческа интерпретация на литературния материал

Дисертационният труд е в обем от 165 страници, като включва въведение, 5 глави за решаване на формулираните основни задачи, списък на основните приноси, ограничения и бъдеща работа, списъци на фигурите, таблиците и съкращенията, списък на публикациите по дисертацията, списък на известните цитирания и списък на използваната литература. В допълнение са приложени 17 анекса с обем от 153 страници. В дисертационния труд има общо 54 фигури и 33 таблици.

Реализираното литературно проучване е въз основа на 200 литературни източници, като всички са на латиница (в това число и уебсайтове) и повечето са от последните 10 години.

Литературният обзор (Глава 1) е много широк и актуален:

- Обхваща хардуерна сигурност: Trojans, counterfeit ICs, reverse engineering, side-channel, fault attacks.

- Подробно разглежда логическо криптиране и обфускация – XOR/XNOR, MUX, Flip-Flop, layout-level техники, SAT атаки и контрамерки.

- Използва голям брой източници (200 референции), включително водещи автори (Bhunia, Tehranipoor, Rajendran, Sinanoglu и др.).

Има ясно очертани:

- таксономии на атаки и защиты,

- изследователски празнини – липса на единна метрик-ориентирана рамка, малко работи, които свързват AHD/AFS, SAT runtime и реални overhead-и в един deployment алгоритъм.

Дисертацията представя широк, актуален анализ на литературата, която не е просто преписана, а има критичен прочит и логично преминаване към собствената методология (Глава 2 – Глава 3). Кандидатът показва добро владение на съвременни насоки на изследване и интерпретира литературата креативно. Обхватът е изчерпателен за целите на дисертационния труд.

Бих написала, че степента на познаване на състоянието на проблема е много добра, а интерпретацията – творческа и целенасочена към формулираните задачи.

3. Съответствие на избраната методика на изследване с поставената цел и задачи на дисертационния труд

Целта: разработване на нова методология и алгоритъм за оценка и избор на хардуерни логически криптиращи техники за киберсигурност на комуникационни системи.

Основните задачи (по съдържанието на Глава 2 – Глава 5) включват:

- дефиниране на метрики: AHD, AFS, key sensitivity, SAT resistance, power/area/delay overhead;

- разработване на алгоритъм за оценка (Глава 3.2) и блок-схема (Фиг. 21, Фиг. 22);

- симулация на криптиране върху случайни логически схеми и върху ISCAS-85/89 бенчмаркове;

- експериментален сетъп с FPGA (Vivado) за реална верификация;

- анализ на корупционен фактор, deceptiveness и secrecy при multi-bit ключове (Глава 4);

- разработване на Security-Cost Driven Deployment Decision Algorithm (Глава 3.5, Глава 5.3, Глава 5.6).

Методологията е:

- количествена – Python симулации, формални метрики, статистически анализ (AHD/AFS, scaling c key-gate density);

➤ експериментална – VHDL/FPGA имплементации, измерване на power/area/delay;

➤ системна – ясно дефиниран workflow: benchmark netlists → parsing → baseline → encryption → security metrics → performance metrics → SAT proxy → deployment decision.

Има добра връзка между:

- теоретичните дефиниции (формули 3.1 – 3.7, 2.13 – 2.21),
- алгоритмичните стъпки (стъпки 1 – 8 в Глава 3.2),
- и реалните резултати (Таблица 17 – Таблица 22, Фиг. 45 – Фиг. 54).

Бих написала, че методиката отговаря напълно на целта и задачите и е типична за сериозен инженерно-научен труд.

Основната цел на дисертацията е да бъдат разработени хардуерни криптографски модули, изградени върху логически структури, да бъдат внедрени в комуникационни хардуерни системи и да бъде оценена тяхната ефективност чрез ключови показатели като мощност, площ и закъснение. Допълнително се анализира нивото на сигурност на всеки подход чрез метрики като AND, AFS и устойчивост на SAT атаки, както и се предлага нова рамка за оценяване на хардуерно криптиране, приложима към комуникационни подсистеми.

За изпълнение на тази цел са формулирани следните задачи:

1. Дефиниране на логически модули – избор и описание на криптографски логически структури, реализация чрез хардуерни описателни езици и изграждане на среда за оценяване.

2. Анализ на ограниченията – идентифициране на слабости и ограничения в съществуващите хардуерни криптографски решения за комуникационни схеми.

3. Сравнителна оценка – изследване на различни техники за логическо криптиране по отношение на площ, закъснение и енергийна консумация.

4. Избор на оптимален метод – определяне на подхода, който предлага най-добър баланс между сигурност и хардуерна ефективност.

5. Разработване на методология – създаване на систематична рамка за оценяване на хардуерни криптографски техники в комуникационни системи.

6. Валидация на решенията – проверка и потвърждение на резултатите от предложените методи.

Посочените задачи са последователни и подходящо обхватни за докторска работа. Като цяло формулировката на проблема и задачите показват висока научно-приложна актуалност.

Дисертацията очертава изследователския процес и теоретичните основи, необходими за работата. Установяването на методология за инженерно проучване изисква структуриран подход, който ефективно разглежда изследователските въпроси, хипотези или постановки на проблемите. Методологията на дисертацията следва ясна логическа последователност, а експерименталните изследвания се основават на предварително разработена методология.

Целта и задачите, формулирани от докторанта, съответстват на изискванията за дисертация за придобиване на образователната и научна степен „Доктор“.

4. Кратка аналитична характеристика на естеството и оценка на достоверността на материала, върху който се градят приносите на дисертационния труд

Материалът включва:

- Python-базирани симулации върху случайни логически схеми и ISCAS бенчмаркове.
- VHDL RTL имплементации на трите криптиращи техники (XOR/XNOR, MUX, Flip-Flop) и тестбенчове (описани в приложенията – Annex 1.9 – 1.16).
- FPGA експериментален сетъп (Vivado 2014.4) за реално сравнение на оригинална и криптираща схема (Фиг. 23 – Фиг. 27).
- Подробни таблици с резултати:
 - AHD/AFS по бенчмарк и метод (Таблица 17),
 - SAT runtime (Таблица 18),
 - комбинирани security/performance метрики (Таблица 19 – Таблица 22),
 - composite Security Score и deployment thresholds (Таблица 22, Таблица 23).

Данните са консистентни: Flip-Flop-базираното криптиране систематично дава:

- най-висок AHD,
- най-нисък AFS,
- най-дълъг SAT runtime (вкл. timeout > 10 000 s за s5378),
- но и най-голям power/area/delay overhead.

Това е логично и добре аргументирано в текста. Като цяло базата е достоверна и достатъчно богата, за да носи тежки изводи.

5. Научни и/или научно-приложни приноси на дисертационния труд

В представената дисертация докторантът е формулирал приноси от научен, научно-приложен и приложен характер. Приемам приносите, но според мен те могат да бъдат обобщени и класифицирани като научно-приложни и/или приложни. Аз бих ги формулирала така (и леко групирала):

Научно-приложни приноси

1. Единна рамка за оценка на логическо криптиране

- Разработена е комплексна методология за оценка на логически заключени схеми, която комбинира:
 - функционална корупция (AHD),
 - fault устойчивост (AFS),
 - key sensitivity,
 - SAT resistance,
 - и хардуерни overhead-и (power, area, delay).
- Това надгражда класически подходи, които често разглеждат само една метрика.

2. Алгоритъм за оценка и сравнение на криптиращи техники

➤ Предложен е формален алгоритъм (Глава 3.2, Фиг. 21 – Фиг. 22) за:

- интегриране на криптиране в схема,
- функционална верификация,
- security/performance анализ,
- и сравнителна оценка на XOR/XNOR, MUX и Flip-Flop криптиране.

3. Доказване на предимствата на Flip-Flop-базираното, state-dependent криптиране

➤ Експериментално е показано, че Flip-Flop-базираното криптиране:

- дава най-висок AHD (до ~0.52–0.56),
- най-нисък AFS,
- и най-висока SAT устойчивост (timeout за s5378).

➤ Особено силен ефект при последователни ISCAS-89 схеми, където състоянието усилва сигурността.

4. Composite Security Score и deployment thresholds

➤ Въведен е композитен показател за сигурност (Security Score /100), който агрегира AHD, AFS, key sensitivity и SAT proxy.

➤ Дефинирани са прагове за:

- Low / Moderate / High / Very High / Critical security,
- и съответно препоръчани платформи (FPGA vs ASIC) и key-gate плътности (Таблица 22).

5. Security-Cost Driven Deployment Decision Algorithm

➤ Разработен е алгоритъм за вземане на решение за внедряване (Глави 3.5, 5.3, 5.6), който:

- използва AHD, AFS, SAT runtime и Composite Security Score,
- избира между XOR/MUX/Flip-Flop,
- и между FPGA и ASIC, според изискваното ниво на сигурност и допустим overhead.

6. Анализ на scaling с key-gate density

➤ Систематично е изследвано влиянието на 2, 5, 10 и 16 key-gates върху:

- AHD, key sensitivity, AFS,
- power/area/delay overhead,
- и Composite Security Score (Фиг. 45 – Фиг. 54).

➤ Показано е, че:

- сигурността расте монотонно с броя key-gates,
- последователните схеми (s5378) печелят най-много,
- но цената в мощност/площ също нараства предвидимо.

Приложни приноси

7. Benchmark-базирана валидация върху ISCAS-85/89

➤ Рамката е приложена върху стандартни бенчмаркове (c432, c499, c880, c1355, s298, s344, s349, s5378), което:

- гарантира възпроизводимост,
- и прави резултатите сравними с други изследвания.

8. Реален FPGA експериментален сетъп

- Разработен е експериментален стенд (Фиг. 23 – Фиг. 27) за:
 - сравнение на оригинална и енкриптирана схема,
 - наблюдение на грешки при грешен ключ,
 - и оценка на слабости на „наивно“ XOR криптиране (примерът с 75 % правилни изходи дори при грешен ключ).

9. Синтезируеми VHDL модели

- Създадени са готови за имплементация VHDL модули за трите енкрипционни техники и тестбенчове, които могат да се използват:
 - в бъдещи изследвания,
 - и в практическо проектиране на защитен хардуер.

Представените приноси имат съществено значение, защото позиционират дисертацията в пресечната точка между научното развитие и практическото приложение в областта на хардуерната сигурност. Тяхната същност най-точно се вписва в категориите научно-приложни и приложни, тъй като:

- предлагат нови методологии и алгоритми, които имат теоретична стойност, но са директно приложими в реални хардуерни системи;
- осигуряват експериментална валидация, която прави резултатите проверими, възпроизводими и полезни за индустрията;
- създават инструменти и модели, които могат да бъдат използвани от други изследователи и инженери.

6. Оценка за степента на личното участие на дисертанта в приносите

В дисертацията са изброени множество публикации в конференции, в които кандидатът е първи автор или съавтор, а документираните реализации показват практическо развитие. Обхватът и съгласуваността на работата предполагат значително лично участие в техническата част. Списъкът с публикациите, свързан с темите на дисертацията, подкрепя висока степен на личен принос от докторанта.

Според текста на дисертацията и приложенията към нея, докторантът е:

- разработил Python симулационната рамка,
 - описал и имплементирал VHDL модулите и тестбенчовете,
 - провел симулации и FPGA експерименти,
 - формулирал Composite Security Score и deployment алгоритъма,
 - и е първи автор на основните публикации по темата (съгласно LIST OF PUBLICATIONS – 10 публикации, голяма част IEEE/Scopus).
- Личното участие може да се оцени като **високо и водещо**.

7. Преценка на публикациите по дисертационния труд: брой, характер на изданията, в които са отпечатани. Отражение в науката – използване и цитиране от други автори

В списъка с публикации са посочени 10 публикации, свързани с темата:

➤ IEEE конференции (TELECOM, TechDefense, IWSSIP и др.) – логическо криптиране, експериментален сетъп, secrecy с multi-bit ключове, алгоритмична рамка.

➤ Книга/глава (IOS Press) за хардуерни решения за киберсигурност на критична инфраструктура.

➤ Част от публикациите вече имат цитирания (посочени в LIST OF CITED PAPERS).

Изданията са реномирани, индексирани в Scopus/IEEE Xplore, което е напълно достатъчно за докторска дисертация в това направление.

Считам, че методите и средствата, разработени от докторанта, имат потенциал да бъдат комерсиализирани.

Основните постижения и резултати от дисертацията са публикувани в 10 научни публикации, разпределени по вид, както следва:

➤ Глава от книга, индексирана в Scopus – 1 брой (№ 5, в Monitoring and Protection of Critical Infrastructure by Unmanned Systems);

➤ Публикации в международни конференции и сборници на конференции, индексирани в IEEEEXPLORE, Scopus и/или Web of Science – 6 броя, както следва: № 1 и № 2 в сборници на National Conference with International Participation (TELECOM) (Sofia, Bulgaria, 2020 г. и 2021 г.), № 3 в сборник IWSSIP на International Conference on Systems, Signals and Image Processing (Sofia, Bulgaria, 2022 г.), № 6 и № 7 в сборник на IEEE International Workshop on Technologies for Defense and Security (TechDefense) (Rome, Italy, 2023 г.), № 8 в сборник на IEEE International Workshop on Technologies for Defense and Security (TechDefense) (Naples, Italy, 2024 г.).

➤ Публикации в международни конференции и сборници на конференции, които очакват индексирание в IEEEEXPLORE, Scopus и/или Web of Science, но към момента не са – 2 броя, както следва: № 9 и № 10 в сборник на IEEE International Workshop on Technologies for Defense and Security (TechDefense) (Rome, Italy, 2025 г.).

➤ Публикация в международни конференции и сборници на конференции – 1 брой, както следва: № 3 в сборника на International Conference on Science, Technology, Business and Innovation of UBT assembles in Kosovo (2021 г.).

От тези 10 публикации докторантът има само една самостоятелна публикация (№ 10), седем са в съавторство само с научния ръководител (№ 1, № 2, № 3, № 6, № 7, № 8, № 9), като докторантът е на първо място и две са в съавторство с трети учен (№ 4, № 5), като от тях докторантът е на първо място в една от тях (№ 4). Всичко това показва, че получените в дисертационния труд резултати са личен принос на докторанта.

Докторантът е представил списък с 5 известни цитирания, като в Scopus са видими 3 цитирания. Препоръчвам на докторанта да конкретизира къде са видими тези цитати. Освен това, бих могла да допълня:

➤ Съгласно Scopus, публикация № 1 има два цитата. А в Google Scholar е виден още един (от Бразилия).

➤ Публикация № 3 има 1 цитат.

➤ Публикация № 5 – според докторантката има 3 цитата, но не е конкретизирано къде са. Не са видими нито в Scopus, нито в Google Scholar.

8. Използване на резултатите от дисертационния труд в научната и социалната практика. Наличие на постигнат пряк икономически ефект и пр. Документи, на които се основава твърдението

Резултатите имат пряка приложимост:

- за дизайнери на сигурен хардуер – избор на криптираща техника и платформа според измерими метрики;
- за FPGA/ASIC проекти в комуникационни и критични системи;
- за академична среда – VHDL моделите и ISCAS-базираните експерименти са подходящи за лабораторни упражнения по хардуерна сигурност.

Пряк икономически ефект не е количествено оценен, но потенциалът е очевиден – по-добре защитен IP, по-малък риск от пиратство и атаки.

9. Оценка на съответствието на автореферата с изискванията за изготвянето му, както и на адекватността на отразяване на основните положения и приносите на дисертационния труд

Представеният автореферат е с обем от 32 страници. Като структура е оформен съгласно изискванията на нормативните документи и представя основните глави на дисертационния труд, както и обобщените приноси. Отразени са апробациите на получените резултати. Номерацията на фигурите и таблиците в автореферата съответства на тези в дисертацията.

10. Мнения, препоръки и бележки.

Нямам съществени коментари по дисертацията. Препоръките и забележките, направени от мен в предварителното мнение, както и на предварителното обсъждане на дисертационния труд, са изпълнени до голяма степен. Препоръчвам на докторанта, в бъдещата си научна и преподавателска дейност, да засили публикациите си в системите Scopus и Web of Science, както и в списания с импакт фактор.

11. Заключение с ясна положителна или отрицателна оценка на дисертационния труд

В заключение, дисертационният труд:

- е актуален, добре мотивиран и ясно структуриран;
- предлага цялостна, метрик-ориентирана рамка за оценка на логическото криптиране;
- съдържа съществени научно-приложни приноси в областта на хардуерната сигурност;
- е подкрепен с достатъчен брой публикации в реномирани издания;

➤ показва висока степен на самостоятелна работа от страна на докторанта.

Представеният дисертационен труд отговаря на изискванията на Закона за развитие на академичния състав в Република България и Правилника за неговото прилагане, а също така и на Процедурните правила за придобиване на научни степени и заемане на академични длъжности на Технически университет, София. Давам положителна оценка на дисертационния труд и предлагам на **маг. Ериселда**

Малай да бъде присъдена образователната и научна степен „доктор“ по научната специалност „Автоматизация на инженерния труд и системи за автоматизирано проектиране“, професионално направление 5.3. Комуникационна и компютърна техника.

Дата: 03.09.2026 г.

.....
/доц. д-р Адриана Бороджиева/

DTK 78-He1-099
03.09.2026

REVIEW

on a dissertation work for the acquisition of an educational and scientific degree "Doctor" (PhD)

Scientific area: 5.3. "Communication and Computer Engineering"
Doctoral program: "Computer-Aided Engineering and Systems for Design Automation"

Author of the dissertation:

Eriselda [redacted] Malaj

Dissertation topic:

Development of New Hardware Solutions for Cybersecurity of Communication Systems

Assoc. Prof. Eng. Adriana [redacted] Borodzhieva, PhD
University of Ruse "Angel Kanchev", Faculty of Electrical Engineering,
Electronics and Automation, Department of Telecommunications
7017 Ruse, 8 Studentska Str.

1. Relevance of the problem developed in the dissertation work in scientific and scientific-applied terms. Degree and levels of relevance of the problem and specific tasks developed in the dissertation

The dissertation is dedicated to the development and evaluation of new hardware solutions for cybersecurity of communication systems through logical encryption at the scheme level. The research examines three main approaches for logical encryption – XOR/XNOR-based, MUX-based and Flip-Flop-based – and analyzes their efficiency, resistance to attacks and applicability in communication-oriented hardware.

The topicality of the topic is determined by several key factors:

- **the globalized production of integrated circuits**, which increases the risk of piracy, overproduction and substitution of intellectual property;
- **real hardware threats**, including reverse engineering, fault injection, side-channel analysis and SAT-based attacks, which bypass traditional software protection mechanisms;
- **the growing need for hardware-level protection** in communication, embedded and critical systems, where compromising the hardware leads to serious functional and security consequences.

The dissertation formulates a clear scientific focus: logical encryption as a means of protecting digital communication circuits. The research emphasizes:

- functional obfuscation, assessed by Average Hamming Distance (AHD);

- resistance to errors and attacks, measured by Average Fault Sensitivity (AFS) and fault-based analysis;
- SAT-resistance of encrypted architectures;
- hardware indicators such as power, area and delay;
- deployment decision algorithm for FPGA and ASIC platforms according to the measured metrics.

The problem is scientifically and scientifically significant, as it is based on established theoretical foundations – logical locking, SAT attacks, ISCAS benchmarks – and leads to practical guidelines for protecting real communication subsystems.

The structure of the dissertation is logical and consistent:

Chapter 1 presents an in-depth review of the existing literature in the field of hardware security, logical encryption and obfuscation, outlining the gaps in current approaches.

Chapter 2 describes the theoretical basis, attack models and the scientific methodology used, including security metrics and design tools.

Chapter 3 discusses the design and implementation of the cryptographic modules, architectural solutions and key management strategies.

Chapter 4 presents the simulation environment, the benchmarks used and the results of the security and hardware performance evaluation.

Chapter 5 analyzes the obtained results, assesses the trade-offs between security and hardware efficiency and examines the robustness of the proposed techniques against various types of attacks.

The conclusion summarizes the main contributions and outlines directions for future work, including issues related to scalability and protection of next-generation integrated circuits. The appendices contain additional materials, program code and experimental data that support the main research.

The formulated goals and objectives are consistent, scientifically justified and fully consistent with current trends in hardware security. All this determines the high scientific and scientific-applied significance of the problem under consideration.

2. Degree of knowledge of the state of the problem and creative interpretation of the literary material

The dissertation is in a volume of 165 pages, including an introduction, 5 chapters for solving the formulated main tasks, a list of main contributions, limitations and future work, lists of figures, tables and abbreviations, a list of publications on the dissertation, a list of known citations and a list of used literature. 17 annexes with a volume of 153 pages are attached as supplements. There is a total of 54 figures and 33 tables in the dissertation.

The literature study carried out is based on 200 literature sources (references), all of which are in Latin (including websites) and most of which are from the last 10 years.

The literature review (Chapter 1) is very broad and up-to-date:

- It covers hardware security: Trojans, counterfeit ICs, reverse engineering, side-channel, fault attacks.

- It examines in detail logical encryption and obfuscation – XOR/XNOR, MUX, Flip-Flop, layout-level techniques, SAT attacks and countermeasures.
- It uses a large number of sources (200 references), including leading authors (Bhunia, Tehranipoor, Rajendran, Sinanoglu, etc.).

It has clearly outlined:

- taxonomies of attacks and defenses,
- research gaps – lack of a unified metric-oriented framework, few works that connect AHD/AFS, SAT runtime and real overheads in a single deployment algorithm.

The dissertation presents a broad, up-to-date analysis of the literature, which is not simply copied, but has a critical reading and a logical transition to its own methodology (Chapter 2 – Chapter 3). The candidate shows good knowing of contemporary research directions and interprets the literature creatively. The scope is comprehensive for the purposes of the dissertation.

I would write that the degree of knowledge of the state of the problem is very good, and the interpretation is creative and purposeful to the formulated tasks.

3. Correspondence of the chosen research methodology with the goal and tasks of the dissertation work

Goal: development of a new methodology and algorithm for evaluation and selection of hardware logical encryption techniques for cybersecurity of communication systems.

The main tasks (according to the content of Chapter 2 – Chapter 5) include:

- definition of metrics: AHD, AFS, key sensitivity, SAT resistance, power/area/delay overhead;
- development of an evaluation algorithm (Chapter 3.2) and a flowchart (Fig. 21, Fig. 22);
- simulation of encryption on random logic circuits and on ISCAS-85/89 benchmarks;
- experimental setup with FPGA (Vivado) for real verification;
- analysis of corruption factor, deceptiveness and secrecy in multi-bit keys (Chapter 4);
- development of Security-Cost Driven Deployment Decision Algorithm (Chapter 3.5, Chapter 5.3, Chapter 5.6).

The methodology is:

- quantitative – Python simulations, formal metrics, statistical analysis (AHD/AFS, scaling with key-gate density);
- experimental – VHDL/FPGA implementations, power/area/delay measurements;
- systemic – clearly defined workflow: benchmark netlists → parsing → baseline → encryption → security metrics → performance metrics → SAT proxy → deployment decision.

There is a good connection between:

- the theoretical definitions (formulas 3.1 – 3.7, 2.13 – 2.21),

- the algorithmic steps (steps 1 – 8 in Chapter 3.2),
- and the real results (Table 17 – Table 22, Fig. 45 – Fig. 54).

In my opinion, the methodology fully meets the goal and tasks and is typical of serious engineering and scientific work.

The main goal of the dissertation is to develop hardware cryptographic modules built on logical structures, to be implemented in communication hardware systems and to evaluate their effectiveness through key indicators such as power, area and delay. Additionally, the security level of each approach is analyzed through metrics such as AHD, AFS and resistance to SAT attacks, and a new framework for evaluating hardware encryption applicable to communication subsystems is proposed.

To achieve this goal, the following tasks have been formulated:

1. Definition of logical modules – selection and description of cryptographic logical structures, implementation through hardware description languages and construction of an evaluation environment.
2. Constraint analysis – identifying weaknesses and limitations in existing hardware cryptographic solutions for communication schemes.
3. Comparative evaluation – examining different logical encryption techniques in terms of area, delay and energy consumption.
4. Optimal method selection – determining the approach that offers the best balance between security and hardware efficiency.
5. Methodology development – creating a systematic framework for evaluating hardware cryptographic techniques in communication systems.
6. Solution validation – verifying and confirming the results of the proposed methods.

The specified tasks are consistent and appropriately comprehensive for a doctoral thesis. Overall, the formulation of the problem and the tasks demonstrate high scientific and applied relevance.

The dissertation outlines the research process and the theoretical foundations necessary for the work. Establishing a methodology for engineering research requires a structured approach that effectively addresses the research questions, hypotheses or problem statements. The methodology of the dissertation follows a clear logical sequence, and the experimental studies are based on a previously developed methodology.

The goal and tasks formulated by the doctoral student correspond to the requirements for a dissertation for the acquisition of the educational and scientific degree "Doctor".

4. A brief analytical characterization of the nature and assessment of the credibility of the material on which the contributions of the dissertation are built

The material includes:

- Python-based simulations on random logic schemes and ISCAS benchmarks.
- VHDL RTL implementations of the three encryption techniques (XOR/XNOR, MUX, Flip-Flop) and testbenches (described in the annexes – Annex 1.9 – 1.16).

➤ FPGA experimental setup (Vivado 2014.4) for real comparison of the original and encryption scheme (Fig. 23 – Fig. 27).

➤ Detailed tables with results:

- AHD/AFS by benchmark and method (Table 17),
- SAT runtime (Table 18),
- combined security/performance metrics (Table 19 – Table 22),
- composite Security Score and deployment thresholds (Table 22, Table 23).

The data is consistent: Flip-Flop-based encryption systematically gives:

- highest AHD,
- lowest AFS,
- longest SAT runtime (incl. timeout > 10,000 s for s5378),
- but also, the largest power/area/delay overhead.

This is logical and well argued in the text. Overall the base is reliable and rich enough to bear serious conclusions.

5. Scientific and/or scientific-applied contributions of the dissertation work

In the presented dissertation, the doctoral student has formulated contributions of a scientific, scientific-applied and applied nature. I accept the contributions, but in my opinion, they can be summarized and classified as scientific-applied and/or applied. I would formulate them like this (and slightly group them):

Scientific and applied contributions

1. A unified framework for evaluating logical encryption

➤ A complex methodology for evaluating logically locked schemes has been developed, which combines:

- functional corruption (AHD),
- fault resistance (AFS),
- key sensitivity,
- SAT resistance,
- and hardware overheads (power, area, delay).

➤ This builds on classical approaches that often consider only one metric.

2. Algorithm for evaluating and comparing encryption techniques

➤ A formal algorithm has been proposed (Chapter 3.2, Fig. 21 – Fig. 22) for:

- integration of encryption into a scheme,
- functional verification,
- security/performance analysis,
- and comparative evaluation of XOR/XNOR, MUX and Flip-Flop encryption.

3. Proving the advantages of Flip-Flop-based, state-dependent encryption

➤ It has been experimentally shown that Flip-Flop-based encryption:

- gives the highest AHD (up to ~0.52–0.56),
- the lowest AFS,

- and the highest SAT resilience (timeout for s5378).
- Particularly strong effect in sequential ISCAS-89 schemes, where the state enhances security.

4. Composite Security Score and deployment thresholds

- A composite security indicator (Security Score /100) is introduced, which aggregates AHD, AFS, key sensitivity and SAT proxy.
- Thresholds are defined for:
 - Low / Moderate / High / Very High / Critical security,
 - and respectively recommended platforms (FPGA vs ASIC) and key-gate densities (Table 22).

5. Security-Cost Driven Deployment Decision Algorithm

- A deployment decision algorithm has been developed (Chapters 3.5, 5.3, 5.6), which:
 - uses AHD, AFS, SAT runtime and Composite Security Score,
 - chooses between XOR/MUX/Flip-Flop,
 - and between FPGA and ASIC, according to the required level of security and allowable overhead.

6. Scaling analysis with key-gate density

- The impact of 2, 5, 10 and 16 key-gates has been systematically investigated, on:
 - AHD, key sensitivity, AFS,
 - power/area/delay overhead,
 - and Composite Security Score (Fig. 45 – Fig. 54).
- It is shown that:
 - security grows monotonically with the number of key-gates,
 - sequential schemes (s5378) gain the most,
 - but the power/area cost also increases predictably.

Applied contributions

7. Benchmark-based validation on ISCAS-85/89

- The framework is implemented on standard benchmarks (c432, c499, c880, c1355, s298, s344, s349, s5378), which:
 - guarantees reproducibility,
 - and makes the results comparable with other studies.

8. Real FPGA experimental setup

- An experimental stand (Fig. 23 – Fig. 27) has been developed for:
 - comparison of original and encrypted scheme,
 - monitoring of errors with wrong key,
 - and assessment of weaknesses of “naive” XOR encryption (the example with 75 % correct outputs even with wrong key).

9. Synthesizable VHDL models

- Ready-to-implement VHDL modules for the three encryption techniques and testbenches have been created, which can be used:
 - in future research,
 - and in practical design of secure hardware.

The presented contributions are of significant importance because they position the dissertation at the intersection between scientific development and practical application in the field of hardware security. Their essence most accurately fits into the categories of scientific-applied and applied, since:

- they offer new methodologies and algorithms that have theoretical value, but are directly applicable in real hardware systems;
- they provide experimental validation that makes the results verifiable, reproducible, and useful to industry;
- they create tools and models that can be used by other researchers and engineers.

6. Assessment of the degree of the dissertation candidate's personal participation in the contributions

The dissertation lists numerous publications in conferences in which the candidate is the first author or co-author, and the documented implementations show practical development. The scope and coherence of the work suggest significant personal involvement in the technical part. The list of publications related to the topics of the dissertation supports a high degree of personal contribution by the doctoral candidate.

According to the text of the dissertation and its appendices, the doctoral student has:

- developed the Python simulation framework,
 - described and implemented the VHDL modules and testbenches,
 - conducted simulations and FPGA experiments,
 - formulated the Composite Security Score and deployment algorithm,
 - and is the first author of the main publications on the topic (according to LIST OF PUBLICATIONS – 10 publications, most of them IEEE/Scopus).
- Personal participation can be assessed as **high and leading**.

7. Evaluation of the publications on the dissertation work: number, nature of the editions in which they were printed. Reflection in science – use and citation by other authors

The list of publications lists 10 publications related to the topic:

- IEEE conferences (TELECOM, TechDefense, IWSSIP, etc.) – logical encryption, experimental setup, secrecy with multi-bit keys, algorithmic framework.
- Book/chapter (IOS Press) on hardware solutions for cybersecurity of critical infrastructure.
- Some of the publications already have citations (listed in the LIST OF CITED PAPERS).

The publications are reputable, indexed in Scopus/IEEE Xplore, which is quite sufficient for a doctoral dissertation in this field.

I believe that the methods and tools developed by the doctoral student have the potential to be commercialized.

The main achievements and results of the dissertation have been published in 10 scientific publications, distributed by type, as follows:

- Chapter of a book indexed in Scopus – 1 issue (№ 5, in Monitoring and Protection of Critical Infrastructure by Unmanned Systems);

- Publications in international conferences and conference proceedings indexed in IEEEXPLORE, Scopus and/or Web of Science – 6 issues, as follows: № 1 and № 2 in proceedings of the National Conference with International Participation (TELECOM) (Sofia, Bulgaria, 2020 and 2021), № 3 in proceedings of IWSSIP of the International Conference on Systems, Signals and Image Processing (Sofia, Bulgaria, 2022), № 6 and № 7 in proceedings of the IEEE International Workshop on Technologies for Defense and Security (TechDefense) (Rome, Italy, 2023), № 8 in proceedings of the IEEE International Workshop on Technologies for Defense and Security (TechDefense) (Naples, Italy, 2024).

- Publications in international conferences and conference proceedings that are awaiting indexing in IEEEXPLORE, Scopus and/or Web of Science, but are not currently indexed – 2 issues, as follows: № 9 and № 10 in the proceedings of the IEEE International Workshop on Technologies for Defense and Security (TechDefense) (Rome, Italy, 2025).

- Publication in international conferences and conference proceedings – 1 issue, as follows: № 3 in the proceedings of the International Conference on Science, Technology, Business and Innovation of UBT assembles in Kosovo (2021).

Of these 10 publications, the doctoral student has only one independent publication (№ 10), seven are co-authored only with the scientific supervisor (№ 1, № 2, № 3, № 6, № 7, № 8, № 9), with the doctoral student in the first place, and two are co-authored with a third scientist (№ 4, № 5), with the doctoral student in the first place in one of them (№ 4). All this shows that the results obtained in the dissertation are the personal contribution of the doctoral student.

The doctoral student has presented a list of 5 known citations, with 3 citations visible in Scopus. I recommend that the doctoral student specify where these citations are visible. In addition, I could add:

- According to Scopus, publication № 1 has two citations. And in Google Scholar, one more is visible (from Brazil).

- Publication № 3 has 1 citation.

- Publication № 5 – according to the doctoral student, there are 3 citations, but it is not specified where they are. They are not visible in either Scopus or Google Scholar.

8. Use of the results of the dissertation work in scientific and social practice. Presence of achieved direct economic effect, etc.

Documents on which the statement is based

The results have direct applicability:

- for designers of secure hardware – selection of encryption technique and platform according to measurable metrics;

- for FPGA/ASIC projects in communication and critical systems;

➤ for academic environment – VHDL models and ISCAS-based experiments are suitable for laboratory exercises in hardware security.

Direct economic effect has not been quantified, but the potential is obvious – better protected IP, lower risk of piracy and attacks.

9. Assessment of the compliance of the abstract with the requirements for its preparation, as well as the adequacy of reflecting the main points and contributions of the dissertation work

The presented abstract is in a volume of 32 pages. Its structure is designed in accordance with the requirements of the regulatory documents and presents the main chapters of the dissertation work, as well as the summarized contributions. The approbations of the obtained results are reflected. The numbering of the figures and tables in the abstract corresponds to those in the dissertation.

10. Opinions, recommendations and notes

I have no significant comments on the dissertation. The recommendations and remarks made by me in the preliminary opinion, as well as in the preliminary discussion of the dissertation work, have been implemented in a great degree. I recommend that the doctoral student, in her future scientific and teaching activities, increase her publications in Scopus and Web of Science, as well as in journals with an impact factor.

11. Conclusion with a clear positive or negative assessment of the dissertation work

In conclusion, the dissertation work:

- is up-to-date, well-motivated and clearly structured;
- offers a comprehensive, metric-oriented framework for evaluating logical encryption;
- contains significant scientific-applied contributions in the field of hardware security;
- is supported by a sufficient number of publications in reputable journals;
- shows a high degree of independent work on the part of the doctoral student.

The presented dissertation meets the requirements of the Law on the Development of the Academic Staff in the Republic of Bulgaria and the Rules for Its Implementation, as well as the Procedural Rules for the Acquisition of Scientific Degrees and the Occupancy of Academic Positions of the Technical University, Sofia. I give a positive assessment of the dissertation work and offer **M.Sc. Eriselda Malaj** be awarded the educational and scientific degree "Doctor" (PhD) in the Doctoral program: "Computer-Aided Engineering and Systems for Design Automation", Scientific area 5.3. "Communication and Computer Engineering".

Date: 03.09.2026

/Assoc. Prof. Adriana Borodzhieva, PhD/